DOCKET: CU-2556

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Lyal Sidney Collins	)
		)
SERIAL NO:	09/856,283	) Group Art Unit: 2133
		)
FILED:	May 18, 2001	) Examiner: Shewaye Gelagay

TITLE: MESSAGE IDENTIFICATION WITH CONFIDENTIALITY, INTEGRITY, AND SOURCE AUTHENTICATION

AMENDED CLAIMS

1. (original) A method for encoding and transmitting by an originating device of a secure message the method comprising the steps of:

(a) generating by a first process using a device identifier, an application identifier and an application value a message value;

(b) combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value;

(c) applying the secret message value and the message to an encoding process to form a secure message block; and

(d) combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

2. (currently amended) A method according to claim 1, whereby an association of the device identifier, the application identifier, and the application value substantially uniquely identifies the originating device and a purpose of one or more of the message and the application, and ~~a identifier~~ an identifier for the message, such message identification being bound with the message content by virtue of the encoding process.

3. (original) A method according to claim 1, whereby the encoding process in step (c) comprises one or more of:

(e) a symmetric encryption process;

(f) an integrity process using one of keyed hash and symmetric encryption techniques;

(g) a process including both symmetric encryption and keyed integrity; and

(h) including the secret message value in a higher level messaging protocol.

4. (original) A method for reception of a securely transmitted message by a recipient device the method comprising the steps of:

(i) extracting one or more of a device identifier, an application identifier and an application value from a received secure message;

(j) generating by a first process using the device identifier, the application identifier and the application value a message value;

(k) generating, according to a second process using the device identifier and the application identifier one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message;

(l) combining the message value with the one or more secret values, to establish a secret message value;

(m) extracting a secure message block from the secure message; and

(n) applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

5. (original) An apparatus for encoding and transmitting by an originating device of a secure message, the apparatus comprising:

(a) message generating means for generating, by a first process using a device identifier, an application identifier and an application value, a message value;

(b) first combining means for combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value;

(c) application means for applying the secret message value and the message to an encoding means which performs an encoding process to form a secure message block; and

(d) second combining means for combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

6. (original) Apparatus according to claim 5, wherein the encoding means comprises one or more of:

(e) a symmetric encryption means;

(f) an integrity processing means using keyed hash or symmetric encryption techniques;

(g) a keyed-symmetric processing means performing symmetric encryption and ensuring keyed integrity; and

(h) encapsulation means for including the secret message value in a higher level messaging protocol.

7. (original) An apparatus for reception of a securely transmitted message by a recipient device the apparatus comprising:

(i) extraction means for extracting one or more of a device identifier, an application identifier and an application value from a received secure message;

(j) message generation means for generating, by a first process using the device identifier, the application identifier and the application value, a message value;

(k) secret value generating means for generating, according to a second process using the device identifier and the application identifier, one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message;

(l) message value combining means for combining the message value with the one or more secret values, to establish a secret message value;

(m) secure message extraction means for extracting a secure message block from the secure message; and

(n) application means for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

8. (original) A computer program product including a computer readable medium having recorded thereon a computer program for encoding and transmitting by an originating device of a secure message, the program comprising:

(a) message generating steps for generating, by a first process using a device identifier, an application identifier and an application value, a message value;

(b) first combining steps for combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one or more intended recipient devices of the message, to establish a secret message value;

(c) application steps for applying the secret message value and the message to encoding steps which perform an encoding process to form a secure message block; and

(d) second combining steps for combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission, the secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value.

9. (original) A computer program product according to claim 8, whereby the encoding steps in step (c) comprise one or more of:

(e) symmetric encryption steps;

(f) integrity processing steps using one of keyed hash and symmetric encryption techniques;

(g) keyed-symmetric steps performing symmetric encryption and ensuring keyed integrity; and

(h) encapsulation steps for including the secret message value in a higher level messaging protocol.

10. (original) A computer program including a computer readable medium having recorded thereon a computer program for reception of a securely transmitted message by a recipient device the program comprising:

(i) extraction steps for extracting one or more of a device identifier, an application identifier and an application value from a received secure message;

(j) message generation steps for generating, by a first process using the device identifier, the application identifier and the application value, a message value;

(k) secret value generation steps for generating, according to a second process using the device identifier and the application identifier, one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message;

(l) message value combining steps for combining the message value with the one or more secret values, to establish a secret message value;

(m) secure message block extraction steps for extracting a secure message block from the secure message; and

(n) application steps for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

11. (original) A system providing secure communications comprising an originating device and one or more receiving devices, wherein said originating device comprises an apparatus for encoding and transmitting a secure message, the originating device comprising:

(a) message generating means for generating, by a first process using a device identifier, an application identifier and an application value, a message value;

(b) first combining means for combining the message value with one or more first secret values, said secret values being known substantially only to the originating device and one more intended recipient devices of the message, to establish a secret message value;

(c) application means for applying the secret message value and the message to an encoding means which performs an encoding process to form a secure message block; and

(d) second combining means for combining an address with the device identifier, the application identifier, the application value and the secure message block, to form a secure message for transmission said secure message being decodable by the one or more of said intended recipient devices which thereby recover the message, the address, the device identifier, the application identifier and the application value;

and wherein a said receiving device comprises an apparatus for reception of a securely transmitted message, said receiving device comprising:

(e) extraction means for extracting one or more of a device identifier, an application identifier and an application value from a received secure message;

(f) message generation means for generating, by a first process using the device identifier, the application identifier and the application value, a message value;

(g) secret value generating means for generating, according to a second process using the device identifier and the application identifier, one or more secret values known substantially only to an originating device and the one or more intended recipient devices of the message;

(h) message value combining means for combining the message value with the one or more secret values, to establish a secret message value;

(i) secure message extraction means for extracting a secure message block from the secure message; and

(j) application means for applying the secret message value and the secure message block to a decoding process to form the securely transmitted message, this message having been securely transmitted by the originating device.

12. (original) A system according to claim 11;

wherein said originating device comprises:

(k) first processing means;

(l) transmitting means adapted to perform one or more establishing and maintaining communications with a receiving means, said first processing means being adapted to control said transmitting means, and adapted to support features (a) to (d);

wherein a said receiving device comprises:

(m) second processing means; and

(n) the receiving means, being adapted to perform one or more of establishing and maintaining communications in conjunction with said transmitting means, said second processing means being adapted control said receiving means, and further adapted to support features (e) to (j).

13. (original) A system according to claim 12, wherein said originating device comprises one of:

(o) a PC comprising the transmitting means, a smart card reader, the first processing means being responsive to the smart card reader and adapted to control said transmitting means, said originating device further comprising a smart card adapted to interface with the smart card reader, said smart card having on board second processing means which in conjunction with said first processing means are adapted to support features (a) to (d); and

(p) a mobile telephone, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d); and

(q) a set top box, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d); and

(r) a cable modem, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d); and

(s) a personal digital assistant, comprising the transmitting means, the first processing means being adapted to control said transmitting means, and also adapted to support features (a) to (d).